HJ

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/445,132	03/13/2000	AHMET MURSIT ESKICIOGLU	RCA88637	9525

24498 7590 01/19/2005

THOMSON MULTIMEDIA LICENSING INC
JOSEPH S TRIPOLI
PO BOX 5312
2 INDEPENDENCE WAY
PRINCETON, NJ 08543-5312

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 01/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/445,132	ESKICIOGLU ET AL.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 September 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 December 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 have been examined. Applicant amended claim 8 in the amendment filed on September 7, 2004.

Response to Amendment

2. The objection to the title is withdrawn as the amended title is more clearly indicative of the invention to which the claims are directed.

3. The 112, second paragraph rejection to claim 9 is withdrawn as the amendment to the claim overcomes the rejection.

Response to Arguments

4. The following is a response to applicant's arguments on pgs. 8-13 in the amendment filed on September 7, 2004.

5. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning (see Remarks, pg. 10, 2nd full paragraph), it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

6. Regarding applicant's argument that the obviousness rejections fail to provide adequate motivation to combine (see Remarks, pg. 9, 3rd full paragraph-pg. 10, 1st paragraph), examiner disagrees. Digital certificates are standard means of securing a public key, wherein the public key is used in an encryption scheme or for a digital signature, which is textbook knowledge to one of ordinary skill in the art-virtually any communication requiring authentication utilizes digital certificates. See Schneier, pg. 574, section 24.9 ISO Authentication Framework. Furthermore, challenge routines are also standard means of ensuring the identity of a node by an inquisitor. See Schneier, pg. 53, last paragraph. Hence, the motivation to combine stated for the aforementioned limitations are found in the Schneier reference wherein the limitations are defined as being staple techniques used to authenticate one host to another in the art.

7. Regarding applicant's argument that the Schneier reference does not cover the step of a third encrypted message being encrypted by A using B's public key garnered from B's digital signature wherein B decrypts the third encrypted message using B's private key, examiner disagrees. As stated above, digital certificates are standard means to verify public keys as taught by Schneier. Further, Schneier teaches that the encryption method wherein a sender encrypts a message using a receiver's public key and the receiver decrypts the encrypted message using the receiver's private key, and the encryption method wherein a sender encrypts a message using a private key of the sender and the receiver decrypts the message using the public key of the sender are variations of the same theme: in public-key cryptography, the public key is the inverting function of the private key and vice versa. See Schneier, pg. 4-5, Public-key

Algorithms. Further, Schneier distinguishes when the two methods are used: for cases when a digital signature is needed (authentication of the sender), the sender's private key is used to encrypt the message, and for other cases the receivers' public key is used to encrypt the message. See Schneier, pg. 4-5, Public-key Algorithms, especially pg. 5, last paragraph under 'Public-key Algorithms' section.

8. Hence, in view of the preponderance of evidence found in the prior art of Schneier, specifically authentication and key exchange methods, digital certificates, challenge routines and public key cryptograph, claims 1-7 and 10 are found to be unpatentable.

9. Regarding applicant's argument that the prior art of record, Schneier in view of Arnold and Force, does not teach the limitations of claims 8, 9 and 11-20, it is noted that the applicant's arguments are only directed against Arnold and Force and not the teaching of Schneier; one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

10. As such, the prior art of record cover the limitations of claims 8, 9 and 10-20.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1-7 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier Applied Cryptography 2nd Edition (hereinafter Schneier). As per claim 10, Schneier teaches a basic authentication protocol using public-key cryptography to manage communication between two nodes A and B (see Schneier, page 51, 'Key and Message Transmission'). Node B sends two encrypted messages to node A: the first encrypted message comprises the principle message to be exchanged, which is encrypted with a key k, and the second encrypted message comprises the key k encrypted using the public key of A. These two encrypted messages are sent to A, wherein A decrypts the second encrypted message with A's private key to retrieve key k, and then uses key k to decrypt the first encrypted message to retrieve the principle message. Completion of these steps establishes a secure communication channel between the two nodes. In this basic protocol, the step of encrypting key k using A's public key by B wherein the encrypted key k is decrypted by A using A's private key is effectively equivalent to the step of encrypting key k using B's private key by B wherein the encrypted key k is decrypted by A using B's public key (see Schneier, pages 4-5, 'Public-key Algorithms').

13. Although this simple authentication scheme does not disclose the use of a digital certificate to secure a key k, Schneier teaches in a different section steps whereby a node B submits their digital certificate along with an encrypted principle message to a

node A, wherein the digital certificate secures a public key that is used to decrypt the encrypted principle message, which was encrypted using the corresponding private key (see Schneier, pages 576-577, 'Authentication Protocols', steps 1-8). Furthermore, Schneier teaches that digital certificates are part of an entrenched framework (X.509 protocol) to cryptographically secure subject identification and public keys for distribution (see Schneier, pages 575, 'Certificates'). It would be obvious to one of ordinary skill in the art at the time the invention was made for the decrypting key (public key of node B) of the encrypted principle message to be secured by a certificate. Motivation for such an implementation would enable node A to ensure that B's public key and B's subject identification information are valid since the information is verified by a trusted third party as taught by Schneier. This protocol is essential to avoid scenarios wherein an unscrupulous third party poses as node B using bogus public keys.

14. This modified authentication scheme does not further disclose the step of node A submitting the original principle message to node B, whereby through the steps listed above, A compares the decrypted principle message received from B and the original principle message to authenticate B. However, these steps correspond to simple challenge requests and responses initiated by A, returned by B, and verified by A. Schneier teaches challenge protocols as a means to verify that the responder to a message is also the receiver of the message and to ensure messages received from a responder is timely and not a replay of a previous dialogue (see Schneier, page 54, first 4 steps; pages 57-58, 'Yahalom' and Table 3.1, 'Ra, Rb'; page 38, 'Signing Documents

and Timestamps'; page 51, 2nd paragraph). These protocols use identifier information as well as a nonce and/or timestamp to achieve these means. It would be obvious to one of ordinary skill in the art at the time the invention was made to use the principle message as a challenge value to authenticate the identity of node B and the timeliness of the message received from node B. Motivation for such an implementation would enable node A to authenticate node B using standard challenge means as taught by Schneier. Finally, this modified authentication scheme further discloses a final authentication step of A sending to B a third encrypted message comprising the data of B's identification garnered from B's digital certificate and encrypted using A's private key wherein B decrypts the third encrypted message using A's public key (see Schneier, page 577, steps 9-15). As noted above, this final step is effectively equivalent to the third encrypted message being encrypted by A using B's public key garnered from B's digital signature wherein B decrypts the third encrypted message using B's private key. The aforementioned covers claim 10.

15. As per claim 1, it is a method claim corresponding to claim 10 and it does not teach or define above the information claimed in claim 10. Therefore, claim 1 is rejected as being unpatentable over Schneier for the same reasons set forth in the rejection of claim 1.

16. As per claim 2, Schneier covers a method for managing access to a device as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, as

mentioned above, the first message (the original principle message sent from node A to node B) comprises data associated with node A and a timestamp.

17. As per claims 3-6, they are method claims corresponding to claims 2 and 10 and they do not teach or define above the information claimed in claims 2 and 10. Therefore, claims 3-6 are rejected as being unpatentable over Schneier for the same reasons set forth in the rejections of claims 2 and 10.

18. As per claim 7, Schneier covers a method for managing access to a device as outlined above in the claim 6 rejection. In addition, the digital certificate and corresponding public key associated with the subject (node B) is issued by an independent certificate authority (see Schneier, pages 574-575, X.509 framework).

19. Claims 8, 9, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, and further in view of Arnold U.S. Patent No. 5,787,172 (hereinafter Arnold). As per claim 11, Schneier covers a method for managing access between two nodes as outlined above in the claim 1-7 and 10 rejections under 35 U.S.C. 103(a). Although Schneier is silent on the matter of the managing access method being integrated between a service provider, a set-top box, and a smart card, authentication methods utilizing certificates to authenticate between these devices are well known in the art. As an example, Arnold discloses a method for authenticating a cryptographic link between a service provider and a set-top box using a smart card coupled thereto by

means of certificate authentication (see Arnold, Figures 1 and 7A-7C and related text). It would be obvious to one of ordinary skill in the art at the time the invention was made to integrate the method covered by Schneier in a connected system between a service provider and a set-top box authenticated with a smart card as disclosed by Arnold. Motivation for such an implementation would enable services provided by the service provider to be restricted based on user rights and privileges stored on the smart card and actuated by a set-top box.

20. As per claim 8, it is a method claim corresponding to claims 7, 10, and 11 and it does not teach or define above the information claimed in claims 7, 10, and 11. Therefore, claim 8 is rejected as being unpatentable over Schneier in view of Arnold for the same reasons set forth in the rejections of claims 7, 10, and 11.

21. As per claim 9, Schneier covers a method for managing access to a device as outlined above in the claim 8 rejection under 35 U.S.C. 103(a). In addition, Schneier teaches that digital certificates comprise data associated with the certificate authority issuing the certificate and data associated with the validity of the digital certificate (see Schneier, page 574, Figure 24.2, 'Issuer' and 'Signature').

22. Claims 12-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Arnold, and further in view of Force et al. U.S. Patent No. 5,533,123 (hereinafter Force). As per claim 12, Schneier covers a method for managing access

as outlined above in the claim 11 rejection under 35 U.S.C. 103(a). Schneier does not expressly disclose that the smart card comprises a plurality of digital certificates, each certificate containing service provider identification. However, smart cards are conventionally designed to incorporate multiple types of information, including a plurality of certificates, each certificate identifying a distinct service. As an example, Force discloses a smart card having this quality (see Force, col. 3, lines 22-31). It would be obvious to one of ordinary skill in the art at the time the invention was made for the smart card to carry a plurality of certificates, wherein each certificate contains service provider information. Motivation for such an implementation would enable access to a plurality of services using only one smart card.

23. As per claims 13-20, they are method claims corresponding to claims 1-12 and they do not teach or define above the information claimed in claims 1-12. Therefore, claims 13-20 are rejected as being unpatentable over Schneier in view of Arnold and/or Force for the same reasons set forth in the rejections of claims 1-12.

Conclusion

24. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

January 11, 2005